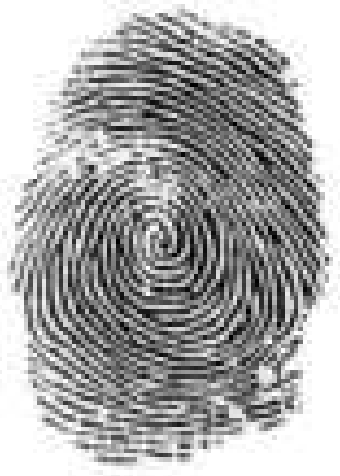
THE NEW TRAFFIC STOP: *"LICENSE, REGISTRATION AND FINGERPRINTS PLEASE."*



By:

Commander Thomas M. Uretsky

Pacific Grove Police Department

California Commission on Peace Officer Standards and Training

May 2007

Command College Class 40

This Command College Independent Study Project is a FUTURES study of a particular emerging issue in law enforcement. Its purpose is NOT to predict the future, but rather to project a number of possible scenarios for strategic planning consideration.

Defining the future differs from analyzing the past because the future has not yet happened. In this project, useful alternatives have been formulated systematically so that the planner can respond to a range of possible future environments.

Managing the future means influencing the future--creating it, constraining it, adapting to it. A futures study points the way.

The views and conclusions expressed in the Command College project are those of the author and are not necessarily those of the Commission on Peace Officer Standards and Training (POST).

©Copyright 2007
California Commission on Peace Officer
Standards and Training

The New Traffic Stop: “License, Registration and Finger Prints Please”

By: Thomas Uretsky, Command College Class 40

Conversations between motorists and officers will be taking an interesting turn in the near future with the implementation of biometric smart cards. Fingerprint smart cards and handheld scanners used by law enforcement are replacing the need for the conventional drivers license. Fingerprint biometrics are rapidly replacing traditional identification cards in both private and government arenas and will soon be the standard for identifying motorists as well. The need to identify, or verify identity has been understood within the criminal justice system for many years. The recording and searching of physical characteristics in support of law enforcement is nothing new, however has not yet been considered as a replacement for physical identification. The new identification system incorporates smart card technology. Smart cards can be used in conjunction with the fingerprint biometric and a PIN to provide three-factor authentication: something you have - the card; something you know - the PIN and something you are - the biometric.

An officer stopping a motorist or making other field contacts will ask for the biometric identification card rather then the traditional identification card or drivers license. The information stored on the card consists of the personal identification of the individual, criminal history, driving history, insurance status,

vehicle and weapons registered to the individual and more. Officers will have more at their fingertips for properly identifying and matching identification to offender then ever before.

By storing an identification template directly on a smart card, law enforcement can also overcome the potential privacy and portability problems of a centrally stored database of templates. Although memory requirements vary between biometric technology vendors, typical template rates are easily managed on a smart card. Taking the privacy discussion a step further, matching algorithms can be implemented on the smart card. This means that instead of reading the template off the card, the biometric is read and given to the card to do the matching in a process known as on-card matching. This technique ensures there has been no tampering with the matching process and also means that the enrolled biometric data never leaves the card. The portability of the biometric enables the card owner to have control of his or her template, while also supporting offline processing.[1]

Essentially officers will have handheld biometric smart card readers that will access the information stored on the smart card and verify it with the biometric fingerprints of the contacted individual. The handheld reader will scan full palm and fingerprints of the person and verifies that the person presenting the card as identification is the same person who submitted their prints when receiving the

[1] Biometric Insight: Finger on the Pulse of Identity. Carl Norell, Gemplus http://www.biometricinsight.com/article1.html

card from the Department of Motor Vehicles, or other issuing agency. The next level of confirmation takes place when the individual is able to enter their personal identification (PIN) number into the reader. The PIN verifies the biometric with the person and then the biometric is sent out wirelessly to the Department of Justice and central warrant section for updated contact information, wants or warrants. Persons who do not have a card in their possession will still be able to enter their PIN and fingerprints and those prints will be transmitted to the Department of Justice for identification.

Identification vs. Verification

What is unique about biometrics is that it is currently the only technology that can indisputably bind a person to an authentication or verification event. Other identity technologies, such as traditional identification cards or drivers licenses bind the event to the card, but not to the person that it was issued to. Because biometrics use unique human characteristics, they are not easily lost, stolen, duplicated or even guessed. It is presently the only way to link a claimed identity to an actual person. There are three basic steps that are taken when using biometrics: enrollment, verification and identification. The first step is the initial enrollment stage when a person's biometric identifiers are captured and stored. The biometric data can be stored in a computer, in a network server or a smart card chip.

In most biometric systems only store reduced digital elements of the biometric feature referred to as a “template.” The second step is the verification of the presented biometric sample against a specific enrolled biometric template. This step verifies whether the person claiming the biometric is actually that person and is called one-to-one matching. The last step is the identification function, or one-to-many matching.

A presented biometric sample is compared to a set of enrolled biometric templates to check if the person is present in the database. In some cases, authentication is achieved by a comparison with a claimed identity. Authentication that incorporates this type of ‘one to-one’ matching is known as verification. Alternatively, authentication might be achieved by comparing a candidate against a group of possible identities, such as the Department of Motor Vehicles or Department of Justice database. In this case, it is the authentication mechanism that decides on the identity. Authentication achieved through a ‘one-to-many’ matching such as this is known as identification.[2]

To create a biometric matching system, a template is created from raw data, such as a fingerprints, and stored for use in either a 'one to one' verification system, or a 'one to many' identification system (where a user's identity is checked against a large database of stored templates). Templates are encrypted

[2] Biometrics and Security – An Introduction By Kevin Shorter & Ian Nice, Trusted Information Management, QinetiQ, http://www.qinetiq.com/home/security/information_and_network_security/white_paper_index.Par.0017.File.pdf

and stored in a central database, as well as on the individual smart card. The template is created when the individual applies for their driver's license, or state issued identification card. Template renewal is every year and can be updated at the local Department of Motor Vehicles office of State Identification Centers, which are centrally located throughout the state. Templates are also updated via auto insurance carriers; tax rolls, property assessment files and other generally accepted public record files. These files verify or confirm last known address and known associate information.

Threats to the System

With the application of the smart card technology and a biometric identification system come an onslaught of possible risks associated with compromising the results. There are unique threats to a smart card biometric authentication system such as the one suggested in this article. The first general threat is the use of a 'false' biometric. The capture device might be fooled into accepting an imitation (usually referred to as a 'false artifact'), or the real thing that has been separated from its owner such as a severed finger. However, any officer accepting a severed finger as a form of identification is more then likely due for retraining.

The second major threat is concerned with modification of the components of the authentication system. The capture device could be modified to output a different

image to the one captured. Alternatively, it could be modified to create a denial-of-service (DOS) that will prevent legitimate users accessing the system (by damaging a reader, for example). The processes of template generation or template matching could be subverted to produce erroneous results; for example, a piece of malicious code could interfere with the template generation software to produce the system attacker's template rather than that of the legitimate user, or the matching process could be modified to produce an artificially high or low matching score.[3]

An ideal form of attack on a biometric system such as this is the template store. If this can be achieved, the attacker will appear to the system to be a legitimate user. Another possibility is to modify the stored template of a particular individual so that they are no longer authenticated by the system (or alternatively, if the system works in identification mode, swap templates around so that one individual is identified as another). Rather than modify the components of the system, an attacker might instead try to subvert the communications between those components. It might be possible to replay old images to the template generator, or old templates to the template matcher, to fool the system into treating an attacker as an individual who has previously been authenticated. It might also be feasible to inject the wrong template into the transmission from the template store to the matching algorithm. Alternatively, the entire template generation and matching process could be effectively bypassed by the insertion

[3] Biometrics and Security – An Introduction By Kevin Shorter & Ian Nice, Trusted Information Management, QinetiQ, http://www.qinetiq.com/home/security/information_and_network_security/white_paper_index.Par.0017.File.pdf

or replay of an erroneous matching score. For each particular scenario, the level of risk posed by the threats listed above is likely to vary.[4]

Reliability of the System

Aside from the obvious and stated threats to the use of a smart card biometric identification system, reliability of the data is also a major concern. False identifications can result in criminals getting away without being detected as well as innocent persons being misidentified. Both of these scenarios can lead to civil actions against officers and departments alike. For example, almost a century after the fingerprints were observed to be distinctive, a 2004 fingerprint contest revealed that fingerprint matching algorithms have false non-match error rate of 2%.[5] If this system were to be deployed in California statewide, given a daily law enforcement contact rate of 200,000 people it would result in 4,000 false rejects every day! While using multiple fingers can significantly reduce the error rate of the fingerprint system, the point is that the error rate even when hackers are not attacking the system is non-zero.

Privacy

Even with all the threats and possibilities of misidentifications a reliable biometric system can provide irrefutable proof of identity of the person contacted by law enforcement. Far more accurate then the current system of drivers licenses and

[4] Automatic Minutiae Detection - http://biolab.csr.unibo.it/Research.asp

[5] FVC2004: Fingerprint Verification Competition, http://bias.csr.unibo.it/fvc2004.

identification cards that are counterfeited, forged, duplicated and issued to non-resident aliens and terrorists. The debate in this research however focuses more on privacy then on misidentifications. Consequently, the users have multiple concerns: Will the undeniable proof of biometrics-based access be used to track the individuals that may infringe upon an individual's right to privacy[6] and anonymity? Will the biometric data be abused for an unintended purpose, e.g., will the fingerprints provided at your local DMV or insurance company be matched against the fingerprints in a criminal database? Will the biometric data be used to cross-link independent records from the same person, e.g., health insurance and grocery purchases? How would one ensure and assure the users that the biometric system is being used only for the intended purpose and none other?

It would appear that the system that meticulously records authentication decisions and the people who accessed the logged decisions using a biometric-based access control system should have a distinct audit trail. Such a system can automatically generate alarms to the users upon observing a suspicious pattern in the system administrator's access of users' logs. While one could stipulate some ingredients of the successful strategy, there are no satisfactory solutions on the horizon for this fundamental privacy problem.[7]

---

[6] Griswold v. Connecticut (381 U.S. 479 1965)

[7] Biometrics: A Grand Challenge *Proceedings of International Conference on Pattern Recognition*, Cambridge, UK, Aug. 2004

Conclusion

Although this article is partial fact and future focused fiction, it is a not to distant reality. As law enforcement capabilities and technology advance so will the need for additional training for officers and increased system security. It is clear that any system assuring reliable person recognition must necessarily involve a biometric component. Because of the unique person identification potential provided by biometrics, they have and will continue to provide useful value by deterring crime, identifying criminals, and eliminating false identifications. At the same time, we will need to be mindful of the need to provide controls to the problem of “function creep”, creating systems that do not threaten basic rights to privacy and anonymity, and substantiate the case for system deployment. Biometrics is one of the most important and more interesting identification applications with its associated unique legal, political and business challenges and it’s coming to a traffic stop near you.